PREPAREDNESS CHECKLIST +

For a Changing Security Landscape

LRS
IT SOLUTIONS

Ways to Keep Your Environment Secure

Today's threat environment means that building in security and operationalizing it across all of your IT, including hybrid cloud environments, is more important than ever.

Modern security means shifting from a strategy that is built around minimizing change to one that is optimized for change. An insight-driven workflow must provide visibility into multiple environments, aggregate information, and take remedial action. Security needs to be an integral component throughout the software delivery pipeline, rather than a disconnected checkbox. LRS IT Solutions can be your partner in this transformation.

In this infographic, we'll discuss today's security landscape and how you can partner with LRS IT Solutions to meet security, risk management, and compliance goals. This includes a preparedness checklist for addressing common, basic requirements for mitigating vulnerabilities, implementing configuration management, and establishing access controls. While these requirements are hardly new, in today's digital world they're amped up for higher threat velocity and volume, IT architectures that are open to the world, and infrastructure that is both heterogeneous and hybrid.

Reasons Why Your Security Policy Could Have Gaps

IT Security is an essential element in any IT infrastructure, from protecting user data against the growing number of threats to ensuring the continuity of the business.

As IT professionals, being able to benchmark, assess threats, and provide our clients with a clear understanding of why a security program is critical to every business is important.

We have created a list of current and significant statistics to provide …

1. The reasons why you need power security tools, processes, and providers in place
2. Insight into the potential sources of the next great security threat
3. A detailed checklist to follow to uncover any gaps or vulnerabilities in your current security strategy.

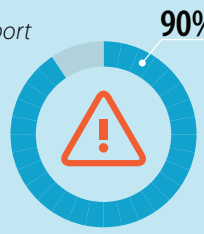
Let's Start with the

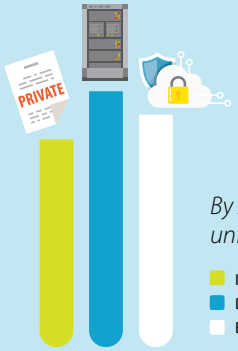
CHANGING IT LANDSCAPE

& Why it Creates Security Challenges for Your Organization

70% of all organizations have at least one app in the cloud

90% of large businesses report major incidents several times a year





By 2021, there will be 3.5 million unfilled cybersecurity jobs

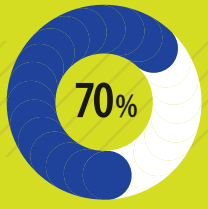
- Information Security
- Data Center Management
- Big Data

And, now let's look at how a

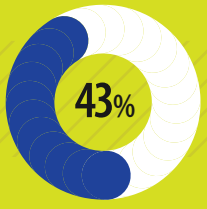
HETEROGENEOUS INFORMATION COLLECTION & STORAGE

could affect security

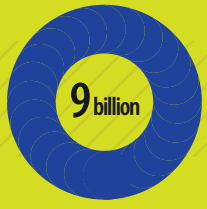
Legacy data must be cleaned up prior to system conversion or integration



of new data centers will use hybrid technology by 2020



of IT departments have concerns on where data is stored



Over 9 billion records have been lost or stolen since 2013

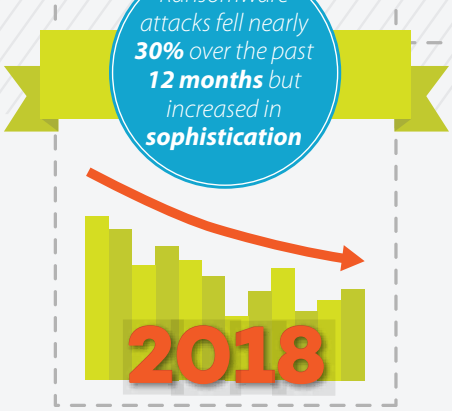
New Threats That You May Not be Prepared For

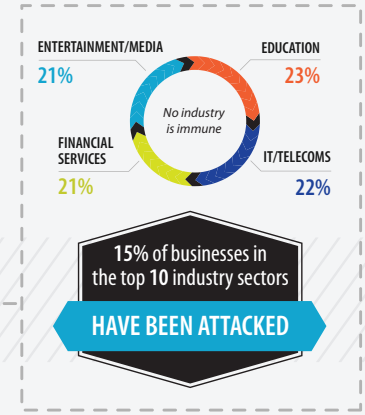
No locale, no industry or organization is bullet proof when it comes to the compromise of data. And it's not just the big fish who are being targeted by cyber criminals. SMEs are equally at risk and are suffering losses as a result.

Here are some of the top security threats and unplanned disasters that took place in the last year and a half. No scare tactics here — just the cold hard facts.

RANSOMWARE IS ON THE RISE...

*Ransomware attacks fell nearly **30%** over the past **12 months** but increased in **sophistication***





*Ransomware attacks are predicted to reach **$11.5 billion annually** by 2019 in global damage costs*

*Ransomware will attack a business **every 14 seconds** by the end of 2019*

*Ransomware attacks on healthcare organizations are predicted to **quadruple by 2020***

NATURAL DISASTER

Could Pose a Greater Threat than Previously Expected

Cybercriminals are known to exploit natural disasters

Hurricanes Harvey and Irma caused between $150 - $200 billion in damage

40% of businesses never reopen after a natural disaster

3 out of 4 companies are unprepared for a natural disaster

HACKERS

are becoming more common-place and bolder

WannaCry and Petya hit global headlines within weeks of each other

There has been a 29% increase in the total cost of data breaches

29%

The average hacker stays hidden in a network for

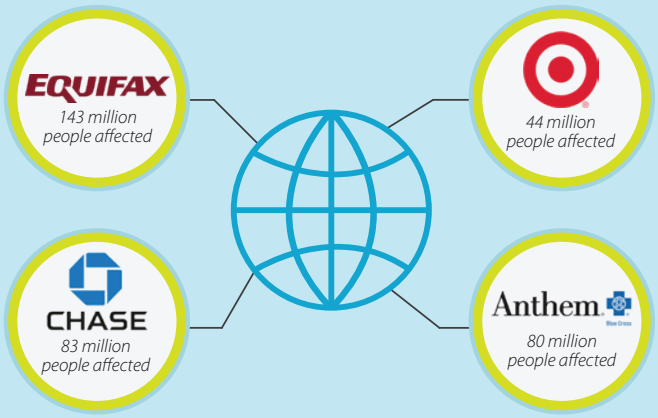
140 days

Cybercrime will cost businesses over $2 trillion by 2019

DATA VOLUMES

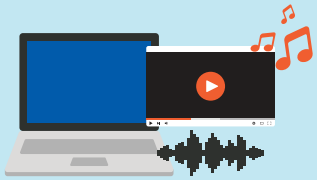
are growing rapidly making it harder to protect and secure them cost effectively

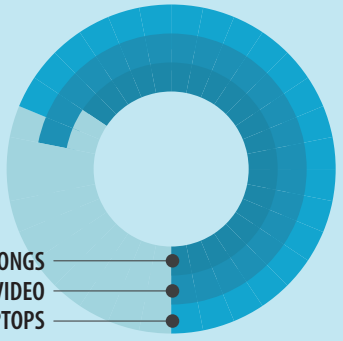
Data production will be 44x greater in 2020 than it was in 2009



The number of records compromised in Q1 and Q2 2018 surpassed the total number of breached records for all of 2017

2.5 Exabytes are produced every day, equivalent to...





530 MILLION SONGS
90 YEARS OF HD VIDEO
5 MILLION LAPTOPS

What You Need to Do Now

Self-Assessment Security Checklist

This checklist evaluates the IT security preparedness of your organization and will better help you determine where there may be gaps you need to address and how to bolster your efforts.

	Yes / No
1. Have you established an enterprise-wide security program?	☐ ☐
2. Do you have any formal written security policies in place?	☐ ☐
3. Have your security policy and processes been reviewed within the past 12 months?	☐ ☐
4. Do you have plans in place to assess new security innovations?	☐ ☐
5. Are your security policies and procedures being followed to the letter?	☐ ☐
6. Have you experienced security breaches at any of your locations within the last year?	☐ ☐
7. Do you regularly assess your current IT security posture and align your security strategy with business goals balancing expense with potential cost of breach?	☐ ☐
8. Besides your auditor, do you have an external advisor to review your security practices?	☐ ☐
9. Are you continually measuring and testing the effectiveness of your security implementations and continuously evolve your security posture to meet emerging threats?	☐ ☐
10. Is your current security program integrated with existing processes to reduce complexity and achieve business results?	☐ ☐
11. Do your system authorities, network settings, exit point settings and port restrictions prevent cyber-attacks?	☐ ☐
12. Are you unable to fulfill requests for security changes or exceptions due to limited resources?	☐ ☐
13. Do you know what the standard level for security breaches is for your industry and geography?	☐ ☐
14. Would you rate your organization's ability to detect, prevent and mitigate threats as excellent?	☐ ☐
15. Do your developers have access to all source/objects they need without wholesale security grants like *ALLOBJ?	☐ ☐
16. Does your Change Management procedure include security reviews?	☐ ☐
17. Are you notified in advance of changes in security policies and laws that affect your organization?	☐ ☐
18. Are you using some form of remote security monitoring service?	☐ ☐
19. Have you created a dedicated budget and a clear vision for the security technologies that can enhance your current posture?	☐ ☐
20. Have you developed a comprehensive sourcing strategy for all security services, and decide which to outsource to third party managed security solutions providers?	☐ ☐
21. Do you work with a partner to fill gaps, particularly using security solutions and services taking into account regulatory, privacy and data protection requirements?	☐ ☐
22. Do you work with partners to better understand the nature of existing and emerging security threats in your business, your industry and at large?	☐ ☐

Security services specialists at LRS IT Solutions can help you evaluate your responses and recommend further steps to ensure successful security strategies for your organization. In business for over 25 years, we offer best of breed, integrated security solutions that protect your networks and critical data assets from compromise. Gain control over your data and the protection of it.

Click here to learn more about our Security Solutions or to schedule a free consultation.

Where to Get Outside Help and How We Can Help You

Security Program Review & Solutions Assessment

When implementing a new security program, look at new solutions and services that will plug today's gaps as well as keep you protected in the future. We specialize in the leading cyber security technologies in the industry. Start out with a program review with one of our security experts.

The Security team at LRS IT Solutions can expand your capabilities by importing results from third-party solutions to provide intelligence and protect your environment attacks. We specialize in the following security services and solutions:

Assessment Services

- *Security Posture Assessment*
- *Recon and Intelligence Gathering*
- *Penetration Testing*
- *Internal Pivot Testing*
- *Data Exfiltration Assessment*
- *User-Awareness Testing/Training*

Security Solutions

- *SIEM*
- *Endpoint Detection and Response*
- *Data Management/Masking*
- *Email Protection*
- *Network Security*
- *Incident Response*

Managed Services

- *Managed SIEM/SOC*

Collaborating with a partner to solve problems is the future of technology. LRS IT Solutions wants to be that partner to provide you with a broad view of security and operationalizing it in a way that makes sense for your business.